

Central Security Operations Center

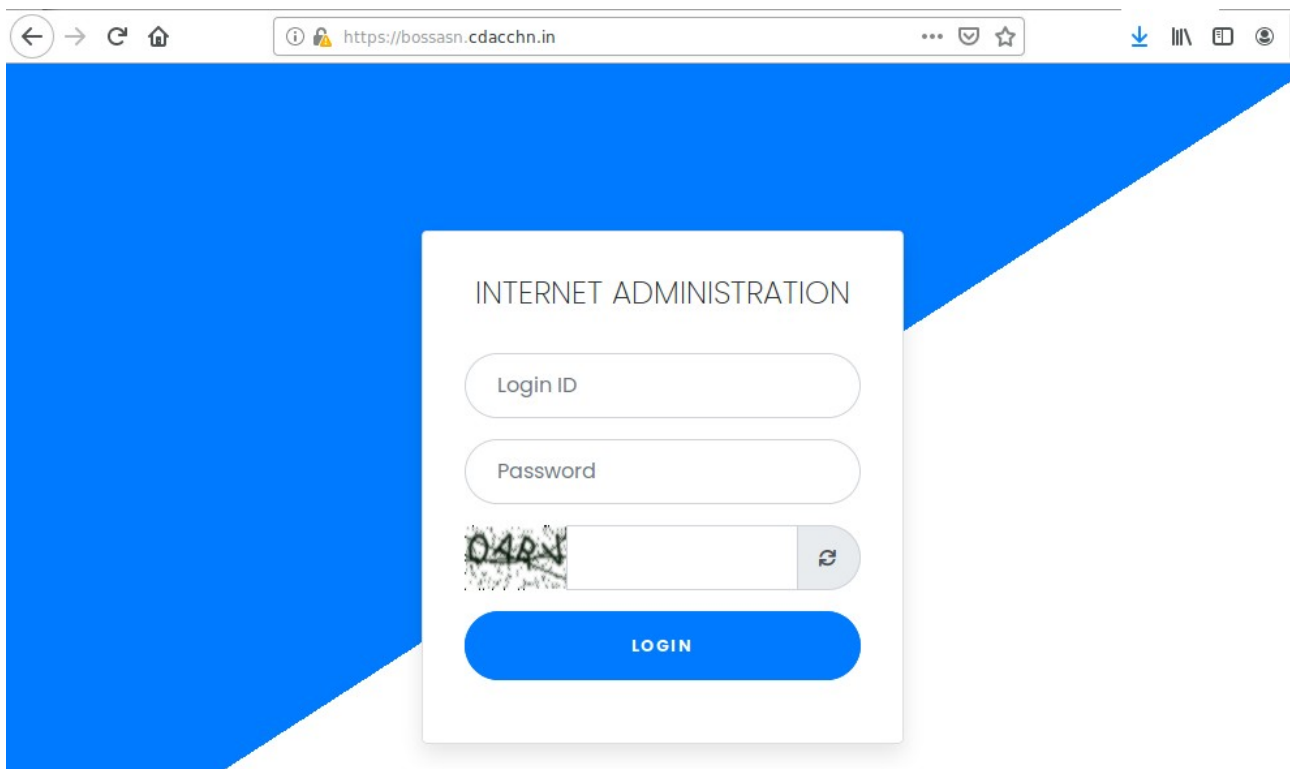
- Administrative Guidance Document

Table of Contents

1. Log In.....	3
2. Dashboard.....	5
3. Generate OTP.....	7
4. Local Admin Creation.....	8
5. Hierarchy Chart.....	13
6.View Client.....	14
7. View Logs.....	15
8.Policy Configuration.....	16
8.1 Adding a Policy.....	17
8.1.1 Services.....	17
8.1.2 Ports.....	17
8.1.3 IP Address.....	17
8.1.4 URL.....	18
8.1.5 Package.....	18
8.1.6 Application.....	19
8.2 Apply/Update Policy.....	19
8.2.1 URLS.....	20
8.2.2 Applications.....	20
8.2.3 Ports.....	21
8.2.4 Services.....	21
8.2.5 IP.....	22
8.3 Exceptional Policy.....	22
8.4 Upload Policy.....	23
9. Client Status.....	24
10. Group.....	30
10.1 Create Group.....	30
10.2 Manage Group.....	31
11. Group Client Mapping.....	31
12. Whitelisting USB Log.....	32
13. View Alerts.....	33
14. Password Reset.....	34

1. Log In

Enter the following URL “<https://bossasn.cdacchn.in>” in the web browser

A screenshot of a web browser displaying the login page for 'INTERNET ADMINISTRATION'. The browser's address bar shows the URL 'https://bossasn.cdacchn.in'. The login form is a white box with a blue header area. It contains three input fields: 'Login ID', 'Password', and a CAPTCHA field with the text '0424'. Below these fields is a blue 'LOGIN' button. The background of the page is blue with a white diagonal stripe.

On entering valid username and password the homepage appears.

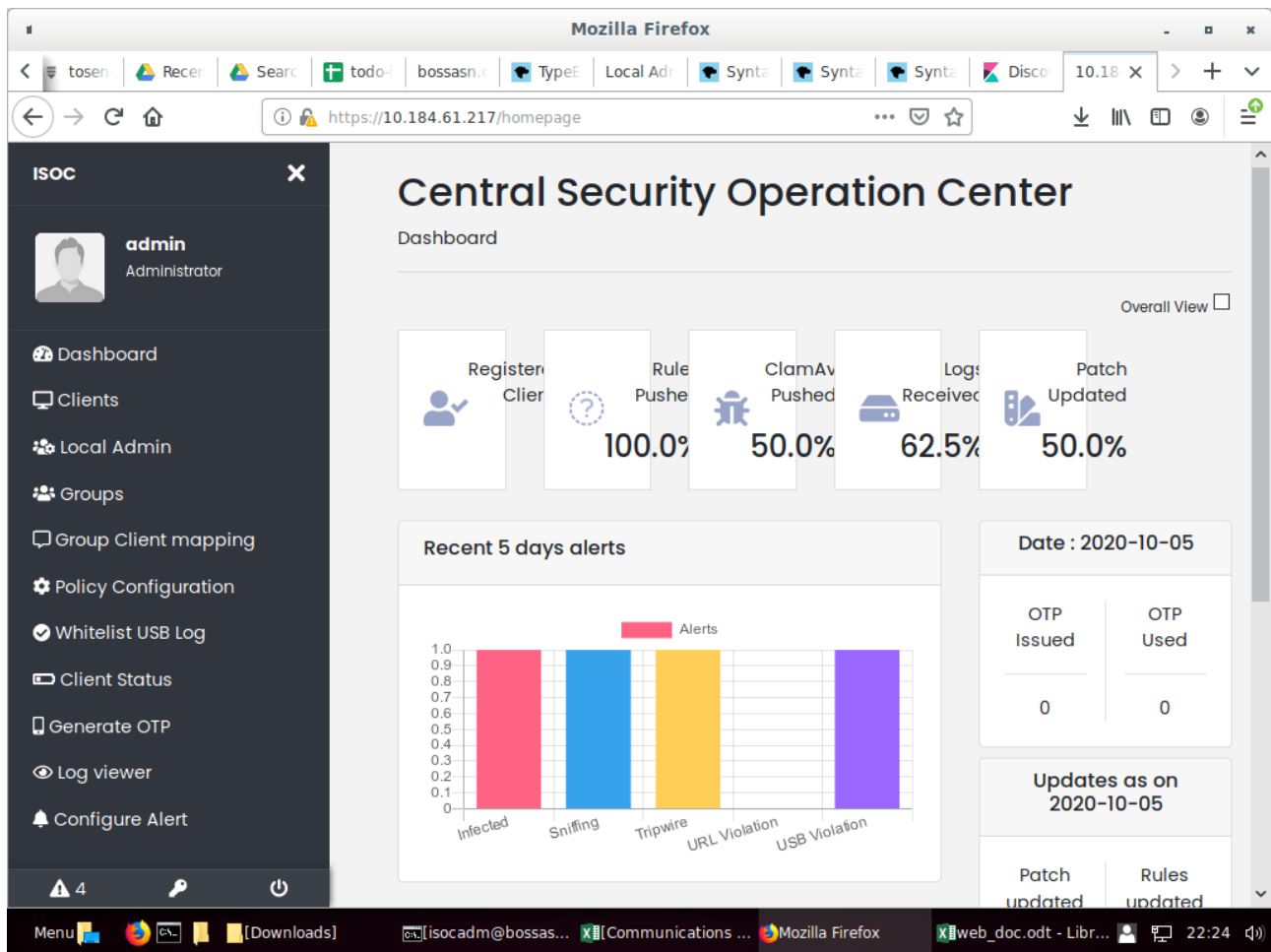
2. Dashboard

Click on “Overall View” to see the stats of all the client machines registered under the unit and its sub-units. If “Overall View” is unchecked the only stats of clients registered under that unit is displayed.

In the dashboard you will find the following statistical data based on the current admin who has logged in

- Registered Client : Count of clients registered
- Rules Pushed: Percentage of clients for which policy is pushed
- Clam Pushed: Percentage of clients for which clam is pushed
- Logs Received: Percentage of clients for which Logs are received

- Patch Update: Percentage of clients for which the Patch Updates are done



- Recent 5 days Alert
 - Alerts of each subcategory that occurred in number of clients for recent 5 days is displayed in the graph.
- OTP Issued
Number of OTPS generated on current date
- OTP Used
Number of OTPS being used
- Patch Updated
Number of Patch updates occurred
- Rules Updated
Number of Clients in which policies are updated

In the dashboard , admin of the AHCC unit is the superuser hence can perform all the actions on the dashboard whereas the other admins can only perform the following operation

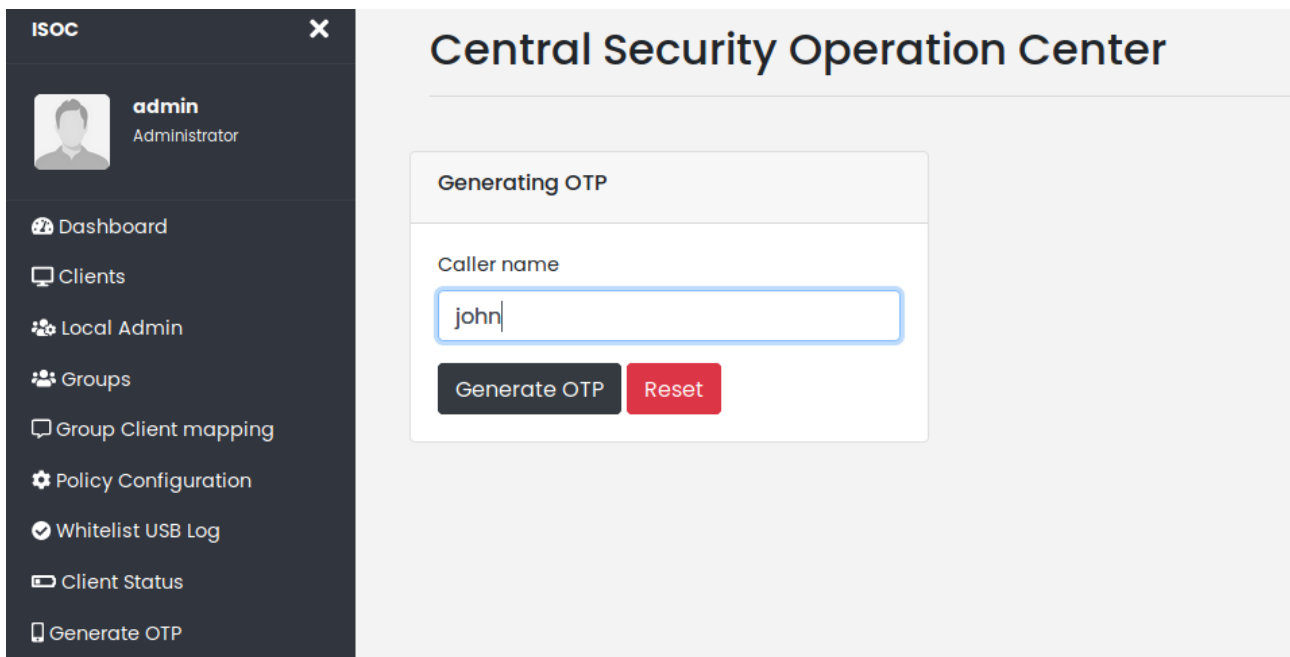
1. Generate OTP

2. Create Local Admin/Unit
3. View Available clients
4. View Logs

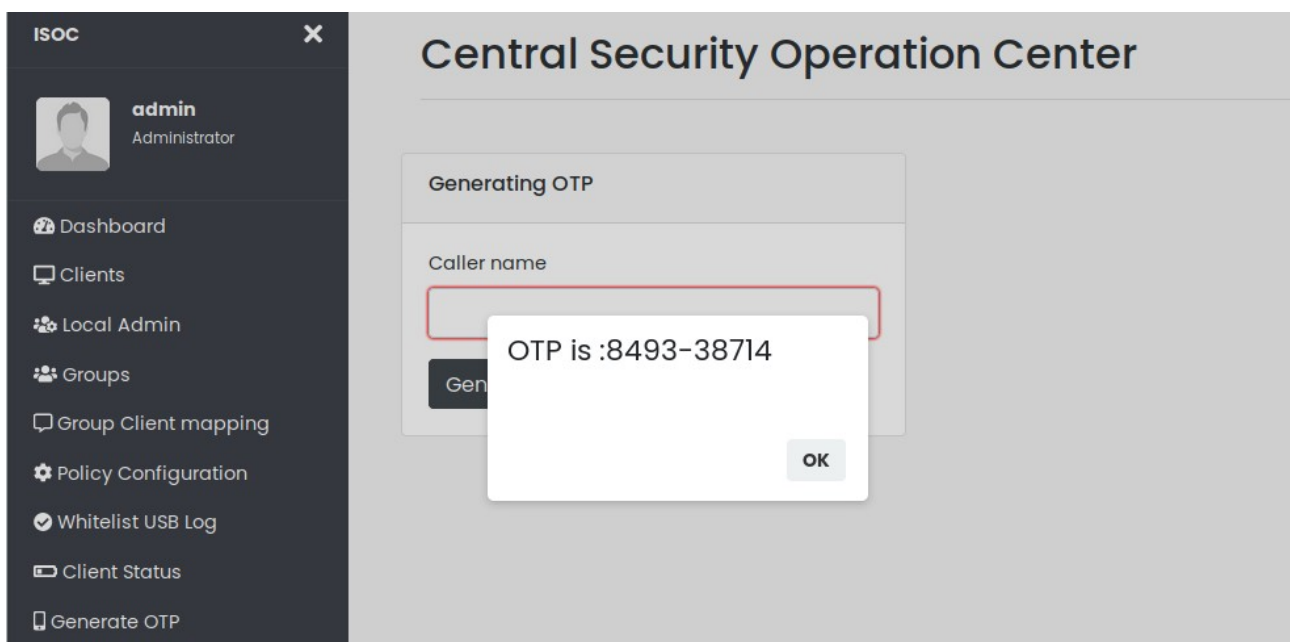
3. Generate OTP

This module is used to generate OTP, that is used during client system registration. The OTP is used to assign the system to the appropriate level in the hierarchy automatically.

Enter the caller name and click “Generate OTP”



Enter the caller name and click on generate OTP .

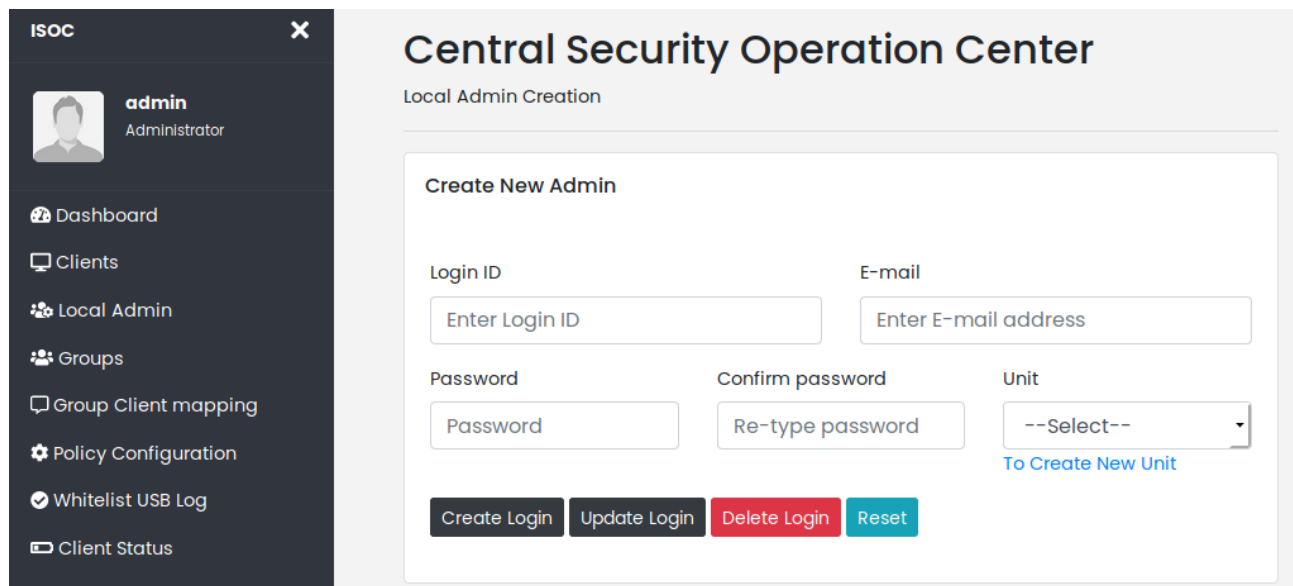


The OTP is generated and displayed on the screen.

4. Local Admin Creation

This module is used to create/update admins login.

The currently logged in admin can create admins one level lower to the current level in hierarchy (i.e a “ecunit” admin can create a “dhimapur” admin within his command).



The screenshot displays the 'Central Security Operation Center' interface for 'Local Admin Creation'. On the left is a dark sidebar with the 'ISOC' logo and a user profile for 'admin Administrator'. The sidebar menu includes: Dashboard, Clients, Local Admin (highlighted), Groups, Group Client mapping, Policy Configuration, Whitelist USB Log, and Client Status. The main content area has the title 'Central Security Operation Center' and subtitle 'Local Admin Creation'. Below this is a 'Create New Admin' form with the following fields: 'Login ID' (text input with placeholder 'Enter Login ID'), 'E-mail' (text input with placeholder 'Enter E-mail address'), 'Password' (text input with placeholder 'Password'), 'Confirm password' (text input with placeholder 'Re-type password'), and 'Unit' (a dropdown menu currently showing '--Select--'). A blue link 'To Create New Unit' is positioned below the Unit dropdown. At the bottom of the form are four buttons: 'Create Login' (dark grey), 'Update Login' (dark grey), 'Delete Login' (red), and 'Reset' (teal).

To create admin, click on “Create Login” and enter the details. Unit can be added by clicking on “To Create New Unit”

For example : When a “AHCC” admin creates a admin for “Eastern Command”. Firstly he creates a new unit named “unit1” and then selects that from the Units drop down list.

ISOC

admin

Extra

Dashboard

Clients

Local Admin

Groups

Group Client mapping

Policy Configuration

Whitelist USB Log

Client Status

Generate OTP

Log viewer

Central Security Operation Center

Create Unit

unit1

Unit for Eastern Command

Add Unit

Reset

Central Security Operation Center

Create Unit

unit1

Unit for Eastern Command

Add Unit

Reset

Unit created sucessfully

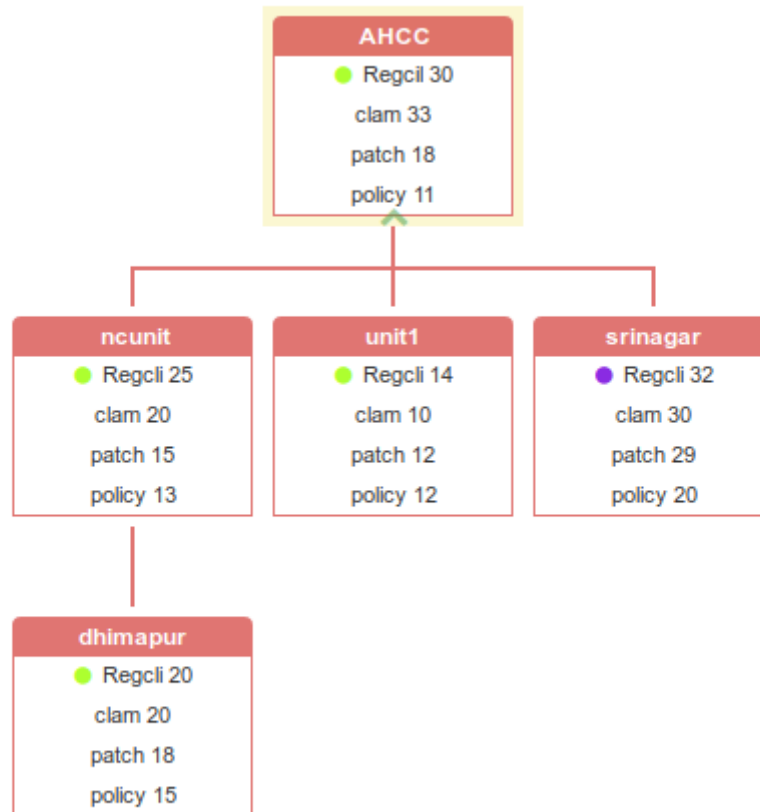
OK

The screenshot shows the 'Central Security Operation Center' interface. On the left is a dark sidebar with the 'ISOC' logo and a user profile for 'admin'. The main content area is titled 'Local Admin Creation' and contains a 'Create New Admin' form. The form has five input fields: 'Login ID' (containing 'ecadmin'), 'E-mail' (containing 'ecadmin@bossasn.in'), 'Password' (masked with dots), 'Confirm password' (masked with dots), and 'Unit' (a dropdown menu showing 'unit1'). Below the 'Unit' dropdown is a blue link that says 'To Create New Unit'. At the bottom of the form are four buttons: 'Create Login' (dark grey), 'Update Login' (dark grey), 'Delete Login' (red), and 'Reset' (teal).

Finally click on “Submit Form”

5. Hierarchy Chart

Clicking on “Hierarchy”, shows the newly added unit unit1 in the hierarchy



6.View Client

To view the list of available client, click on “Clients”

ISOC

admin
Administrator

Dashboard

Clients

Local Admin

Groups

Group Client mapping

Policy Configuration

Whitelist USB Log

Client Status

Generate OTP

Log viewer

Configure Alert

4

Central Security Operation Center

Registered Client List

Show 10 entries

Q

Client Name	Unit	MAC	IP	Reg Status
johnahcc	AHCC	00:0f:fe:d1:04:ba	10.184.36.158	Yes
SAGAR ONE SIX SEP	AHCC	08:00:27:f3:dd:77	10.184.35.85	Yes
Sangeetha	AHCC	08:00:27:cf:03:69	10.184.35.161	Yes
Sangeetha	AHCC	08:00:27:4f:49:a2	10.184.35.161	Yes
Sangeetha	AHCC	08:00:27:0f:fd:41	10.184.35.161	Yes
Sangeetha	AHCC	08:00:27:7a:9f:3c	10.184.35.161	Yes
test one	AHCC	48:0f:cf:50:eb:4a	120.57.114.119	Yes
test two	AHCC	48:0f:cf:51:a4:87	120.57.114.119	Yes

7. View Logs

To view the logs, click on “LogViewer”

Central Security Operation Center

Log Viewer

Unit Name :
AHCC

Clients :
8493-johnahcc-9VY70Y9T-29C

Logs :
ANTIVIRUS SCAN LOG

Log Date :
07 / 01 / 2020 10 / 04 / 2020

*Search Term :

Search

Reset

*Case Sensitive

10 entries

search

Client Host	Log Type	DateTime	Message
No data available in table			

In the window that appears select the Unit and then select the client and from the dropdown list select the logtype and finally click “Search”. To reset click on “Reset”

The selected log gets displayed. To view other logs click on the name of the log

ISOC

admin

Administrator

Dashboard

Clients

Local Admin

Groups

Group Client mapping

Policy Configuration

Whitelist USB Log

Client Status

Generate OTP

Log viewer

Configure Alert

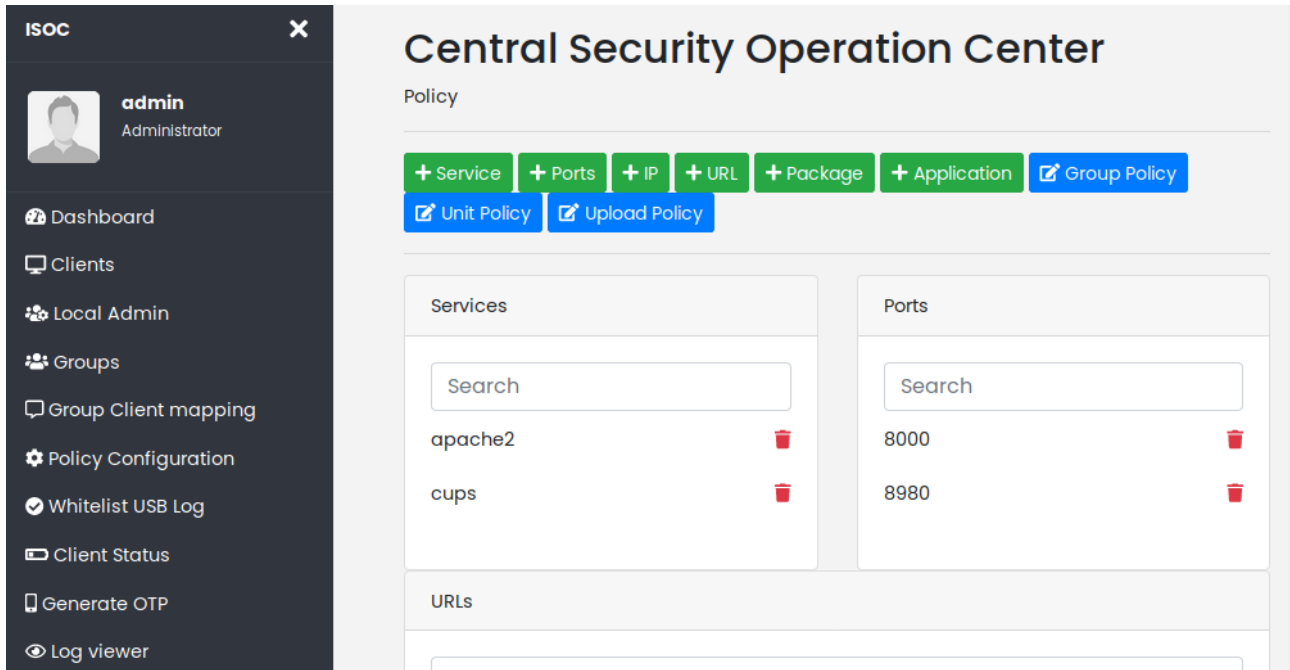
10 entries

search

Client Host	Log Type	DateTime	Message
9VY70Y9T	ANTIVIRUS SCAN LOG	2020-10-04 11:15:01	Knownviruses:8918418,Engineversion:0.102.4,Scanned:239.69,Time:74.062
9VY70Y9T	ANTIVIRUS SCAN LOG	2020-10-04 11:15:01	Infected file is /home/cdaci/Downloads/eicar.com
9VY70Y9T	ANTIVIRUS SCAN LOG	2020-10-04 11:15:01	Infected file is /home/cdaci/Downloads/eicar.com
9VY70Y9T	ANTIVIRUS SCAN LOG	2020-10-04 11:15:01	Infected file is /home/cdaci/Downloads/eicar.co
9VY70Y9T	ANTIVIRUS SCAN LOG	2020-10-04 11:15:01	Infected file is /home/cdaci/Downloads/eicar.com
9VY70Y9T	FILE SYSTEM STATUS	2020-10-04 00:05:02	fs-root:27,fs-home:1,fs-var:9,fs-usr:27,fs-ram-total
9VY70Y9T	ANTIVIRUS SCAN LOG	2020-10-03 11:15:01	Infected file is /home/cdaci/Downloads/eicar.com

8. Policy Configuration

The AHCC admin has this option to set policies for the client machines. Click on “Policy Configuration”



8.1 Adding a Policy

8.1.1 Services

To add a service Click on PolicyConfiguration → +Service

Add Policy ×

Policytype

service

Value

cups

Author

ADMINI

+ Submit

8.1.2 Ports

To add a port Click on PolicyConfiguration → +Ports. Only numbers are allowed for this policytype.

Add Policy ✕

Policytype

ports

Value

1008

Author

ADMINI

+ Submit

8.1.3 IP Address

To add a IP Address Click on PolicyConfiguration → +IP. Only a valid IPV4 address will be allowed.

Add Policy ✕

Policytype

ip

Value

10.184.0.4

Author

ADMINI

+ Submit

8.1.4 URL

To add a URL Click on PolicyConfiguration → +URL

Add Policy ✕

Policytype

url

Value

youtube.com

Author

ADMINI

+ Submit

8.1.5 Package

To add a package Click on PolicyConfiguration → +Package

Add Policy ✕

Policytype

package

Value

apache2

Author

ADMINI

+ Submit

8.1.6 Application

To add a application Click on PolicyConfiguration → +Application

Add Policy ✕

Policytype

application

Value

firefox

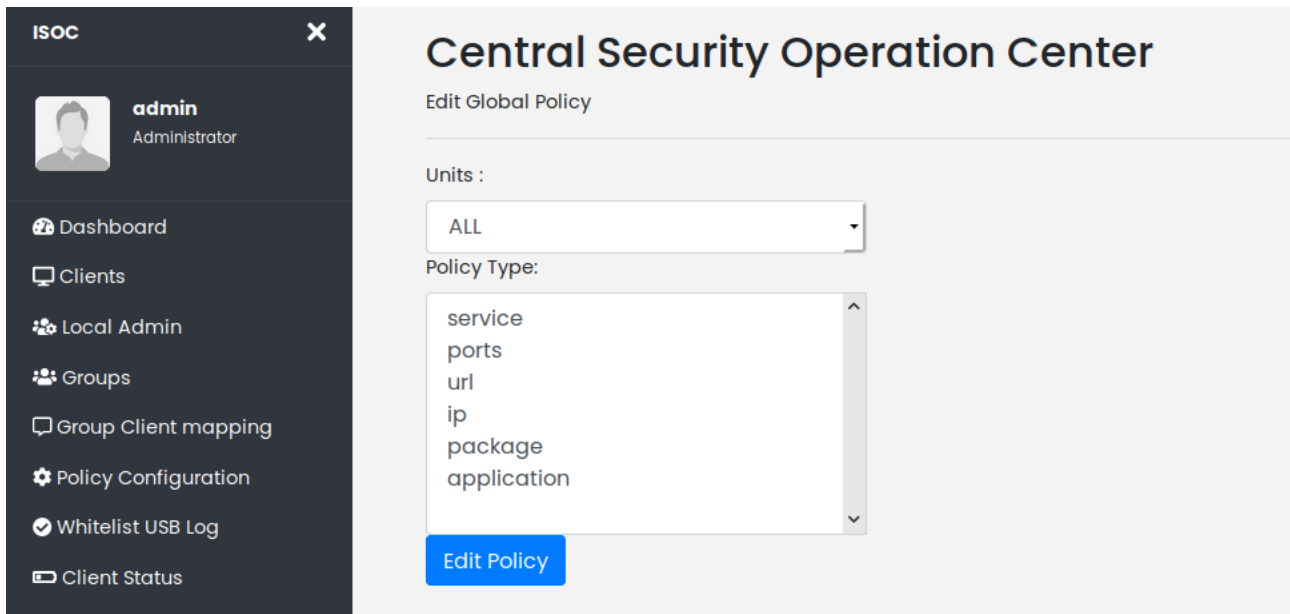
Author

ADMINI

+ Submit

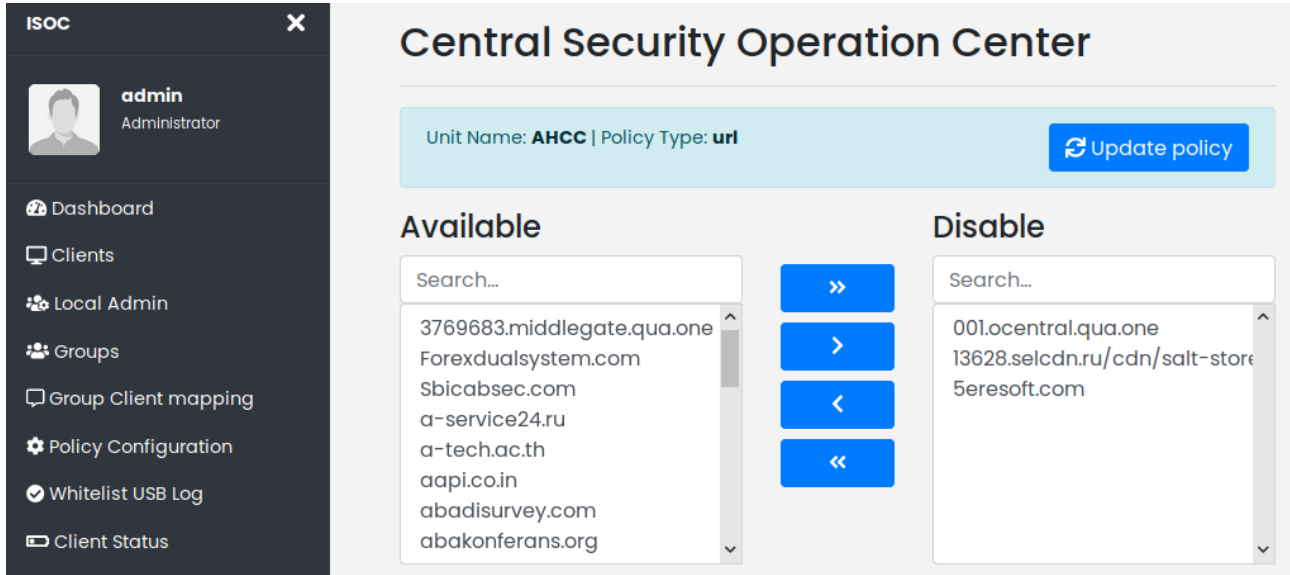
8.2 Apply/Update Policy

To apply policy to the clients , click Policy Configuration → UnitPolicy the following page appears on the screen



8.2.1 URLS

To block a URL, select the “Url” option and click Edit Policy

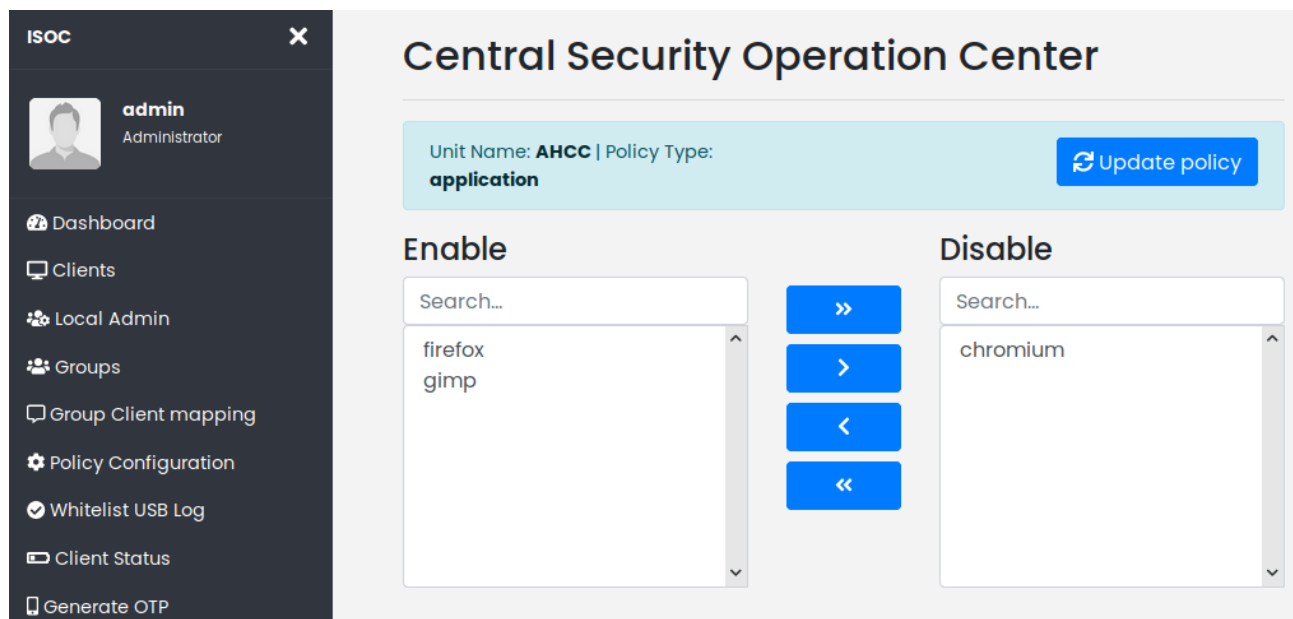


Select one or multiple URLs from the available URLs and click on > key in the form to push it to the disable side , after verifying click on update policy to push the URLs to clients under all the Units. Finally click “Update”.

To unblock a URL, select the URL from the disable list , click on < button to move it to Available list and click “Update”.

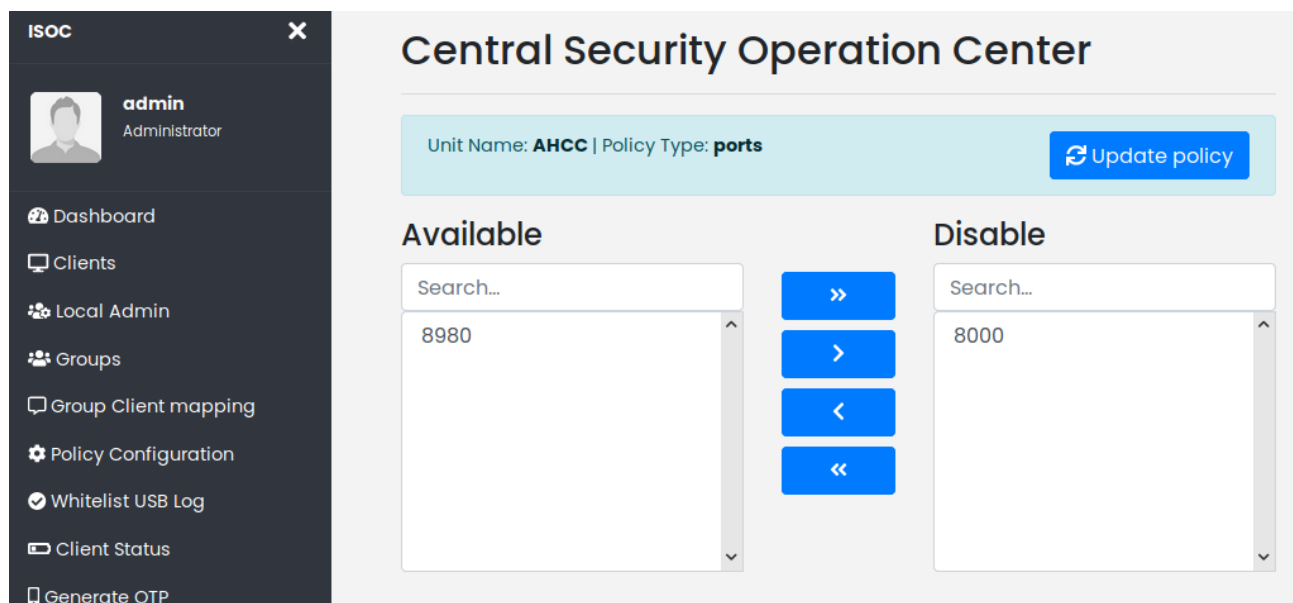
8.2.2 Applications

To disable application in client, select “Application” / Enter the application name search box and click on Search. Select the application from the list and click on > and click “Update Policy”.



8.2.3 Ports

To activate/deactivate port, Select “Edit Global Policy” → “Port” and click “Edit Policy”



Select the port that is to be activated/deactivated and toggle between the Active Ports/Inactive Ports using the >>/<< buttons respectively.

Finally click “Update Policy”

8.2.4 Services

To activate/deactivate port, Select “Edit Global Policy” → “Service” and click “Edit Policy”

The screenshot shows the 'Central Security Operation Center' interface. On the left is a dark sidebar with the 'ISOC' logo and a user profile for 'admin' (Administrator). The sidebar menu includes: Dashboard, Clients, Local Admin, Groups, Group Client mapping, Policy Configuration, Whitelist USB Log, Client Status, and Generate OTP. The main content area has a header bar showing 'Unit Name: AHCC | Policy Type: service' and an 'Update policy' button. Below this, there are two columns: 'Available' and 'Disable'. The 'Available' column has a search bar and a list containing 'apache2'. The 'Disable' column has a search bar and a list containing 'cups'. Between the two columns are four blue buttons: '>>', '>', '<', and '<<'. The 'Available' list has a scrollbar on the right.

Select the service that is to be activated/deactivated and toggle between the Active Services/Inactive Services using the >>/<< buttons respectively.

Finally click “Update Policy”

8.2.5 IP

To activate/deactivate port, Select “Edit Global Policy” → “IP” and click “Edit Policy”

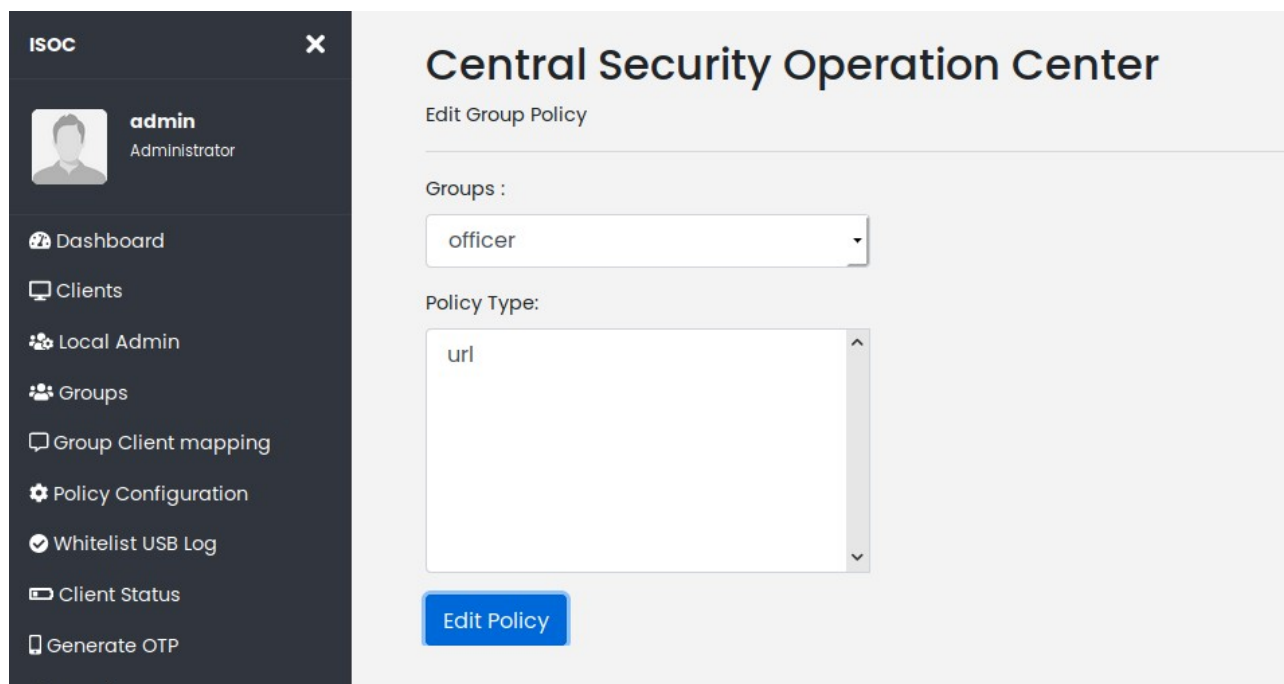
The screenshot shows the 'Central Security Operation Center' interface for IP configuration. The sidebar is identical to the previous screenshot. The main content area header bar shows 'Unit Name: AHCC | Policy Type: ip' and an 'Update policy' button. Below this, there are two columns: 'Available' and 'Disable'. The 'Available' column has a search bar and a list containing the following IP addresses: 10.184.2.140, 10.184.36.112, 10.184.36.201, 10.184.36.216, and 10.184.8.0. The 'Disable' column has a search bar and a list containing the following IP addresses: 10.184.36.110, 10.184.36.212, and 10.184.51.210. Between the two columns are four blue buttons: '>>', '>', '<', and '<<'. The 'Available' list has a scrollbar on the right.

Select the service that is to be activated/deactivated and toggle between the Active IPs/Inactive IPs using the >>/<< buttons respectively.

Finally click “Update Policy”

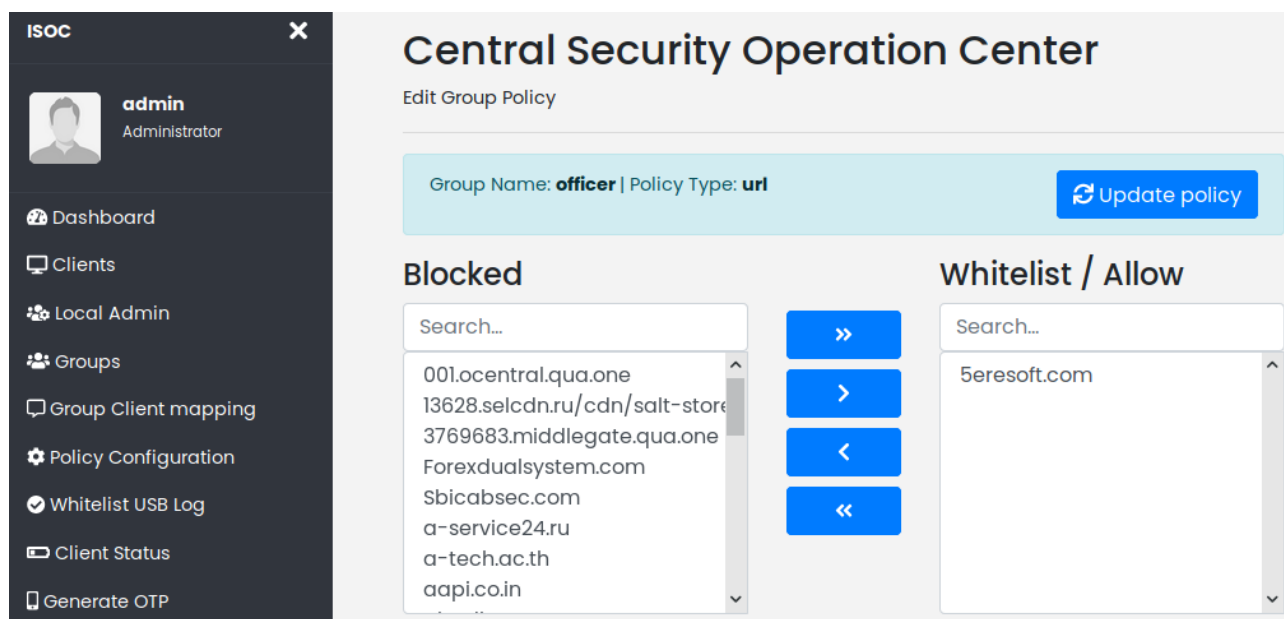
8.3 Exceptional Policy

To add exceptional URL policy(allow URLs to people belonging to a group) click on PolicyConfiguration → Group Policy , the following screen appears.



Select the group and click on edit Policy.

From the list of Blocked URLs , select the url you want to allow for the selected group. For example “5eresoft.com” for officer group and click on Update Policy button to allow the members of officer group to access that URL.



8.4 Upload Policy

To upload policies from a file click on Policy Configuration → Upload Policy. Input a CSV file with policytype,value,author on the first line, the actual values on the subsequent lines.

For example:

```
policytype,value,author
```

```
url,facebook.com
```

```
ip10.184.55.10
```

You can also see a sample CSV by clicking on Show CSV button.

Browse the file and click on upload to load the policies in addition to the already existing policies

Central Security Operation Center

Upload Policy

Click on the button to see a sample CSV:

Show CSV

Browse...




No file selected.

Upload

9. Client Status

The client update status is shown on screen as follows on clicking “Client Status”. We can filter the status unitwise by entering the unitname as shown below.

Client Update Status

   Column Visibility

Show 10 entries


Q

AHCC

Client Name	Unit	Reg Status	Registered	Log	Policy	Clam	Patch
johnahcc	AHCC	Yes	29-09-2020	05-10-2020	30-09-2020	30-09-2020	30-09-2020
SAGAR ONE SIX SEP	AHCC	Yes	17-09-2020	17-09-2020	17-09-2020		
Sangeetha	AHCC	Yes	14-09-2020	16-09-2020	16-09-2020	14-09-2020	16-09-2020
Sangeetha	AHCC	Yes	17-09-2020	26-09-2020	26-09-2020	18-09-2020	18-09-2020
Sangeetha	AHCC	Yes	29-09-2020	30-09-2020	30-09-2020	30-09-2020	30-09-2020
Sangeethat	AHCC	Yes	12-09-2020		14-09-2020		
test one	AHCC	Yes	07-09-2020		28-09-2020		

Central Security Operation Center

Whitelisted USB Log Entries

Name	Whitelist Log Pattern	Date	Action
hp1008	03f0:002a	Sept. 23, 2020	

Add Whitelist Entries

Name

Real Name of user should required

Whitelist Pattern

Pattern for whitelist should required

10. Group

Group menu is only available for AHCC adminuser. It is mainly used for grouping clients for which there is a need to push exceptional policies.

10.1 Create Group






To create a group click on this menu. Enter a Group Name and a short description for the group and click on Add Group to Create group.

The screenshot shows the 'Central Security Operation Center' interface. On the left is a dark sidebar with the user 'admin Administrator' and a menu including Dashboard, Clients, Local Admin, Groups, Group Client mapping, Policy Configuration, and Whitelist USB Log. The main area has a 'Create Group' form with two input fields: 'Group Name' and 'Description: Description about The Group'. Below these fields are 'Add Group' and 'Reset' buttons. A 'Manage Group' link is at the bottom of the form.

10.2 Manage Group

To edit/ update / delete a group click on this menu.

The screenshot shows the 'Manage Group' interface. The sidebar is identical to the previous one. The main area features a 'Manage Group' button, a 'Column Visibility' dropdown, and a table of groups. The table has columns for 'Group Name', 'Description', and 'Action'. It displays two groups: 'officer' and 'exception1'. A search bar and a 'Show 10 entries' filter are also present.

Group Name	Description	Action
officer	officer	  
exception1	exception group	 

11. Group Client Mapping

To map/unmap a client to a exceptional group select a group and select client and use >/< button to assign/unassign a client to the selected group.

Central Security Operation Center

List groups

officer

Action

Unassigned Clients

Search...

4182-chnone
4796-asnchamyseven
4796-chamytezp
4796-dimapurchamyone
6284-Sangeetha
6284-njohn
8197-johnsep
8493-SAGAR ONE SIX SEP

>
<

Assigned Client

Search...

6492-John

12. Whitelisting USB Log

To whitelist USB Log click on “Whitelist USB Log”

Add Whitelist Entries

Name

hp1008

Whitelist Pattern

03fa:002a

Note: Pattern for log entry like "09/17/2017 17:15:48 HUA?WEI TECHNOLOGIES-HUAWEI Mobile, Mass Storage 561a:812b" pattern text must be **561a:812b**

Add Pattern

Reset

Enter the name of USB device and the pattern , the vendor ID is entered as shown above and click Add Pattern.

It will get added like shown below.

Central Security Operation Center

Whitelisted USB Log Entries

Name	Whitelist Log Pattern	Date	Action
hp1008	03f0:002a	Sept. 23, 2020	

Add Whitelist Entries


Name


Whitelist Pattern

13. View Alerts


The Alerts generated for past five days are listed on the Dashboard. Click on Alert symbol “!” to see the list of alerts created in the dashboard.


ISOC








admin
Administrator


 Dashboard


 Clients


 Local Admin

 Groups

 Group Client mapping


 Policy Configuration

 Whitelist USB Log


 Client Status

Central Security Operation Center


List of Notification Found




SOME ONE TRIED TO ACCESS 1 CLIENT(S) REMOTELY IN LAST 5 DAY(S)



CLAMAV FOUND VIRUS / MALWARE IN 1 CLIENT(S) LAST 5 DAY(S)



LOG ABOUT BINARY-FILE INTEGRITY FOUND in 1 CLIENT(S) LAST 5 DAY(S)



USB VIOLATION HAPPENED IN 1 CLIENT(S) LAST 5 DAY(S)

Click on each of the links to find the details

ISOC

admin

Administrator

Dashboard

Clients

Local Admin

Groups

Group Client mapping

Policy Configuration

Central Security Operation Center

List of Violated Client(s)-" SNIFFING LOG "

Column Visibility

Show 10 entries

search

Client Name	Host Name	No.of Violated
8493-johnahcc	9VY70Y9T	1

Showing 1 to 1 of 1 entries

On clicking the search icon the violated log entry appears on the screen

ISOC

admin

Administrator

Dashboard

Clients

Local Admin

Groups

Group Client mapping

Policy Configuration

Whitelist USB Log

Client Status

Generate OTP

Central Security Operation Center

Violated log entries received from client "8493 - johnahcc "

Column Visibility

Show 10 entries

search

Client Host	Log Type	DateTime	Message
9VY70Y9T	SNIFFING LOG	2020-09-30 11:32:15	[62829.670834] IN=enp0s25 OUT= MAC=00:0f:fe:d1:04:ba:00:1f:6c:3d:35:bf:08:00 SRC=10.184.61.206 DST=10.184.36.158 LEN=60 TOS=0x00 PREC=0x00 TTL=62 ID=28647 DF PROTO=TCP SPT=48338 DPT=22 WINDOW=64240 RES=0x00 SYN URG=0


Showing 1 to 1 of 1 entries

14. Password Reset

To reset password of admin, click on the key symbol from the bottom-most menu in the dashboard, the reset password screen appears. Enter old password , new password and click on "Reset Password"

Note: New password should be a combination of alphanumeric and special characters.

ISOC



admin
Administrator

Dashboard

Clients

Local Admin

Groups

Group Client mapping

Policy Configuration

Whitelist USB Log

Client Status

Central Security Operation Center

Current Password:

New Password:

Confirm New Password:

Change Password

Reset

Finally click on “Change Password”.